A secure key distribution system of quantum cryptography based on the coherent state

Guo Guang-can and Zhang Xiao-yu
Physics Department, University of Science and Technology of China, Hefei, Anhui, P.R.China

Abstract

A quantum key distribution based on coherent state is introduced in this paper. Here we discuss the feasibility and security of this scheme.

The cryptographic communication has a lot of important applications, particularly in the magnificent prospects of private communication. As one knows, the security of cryptographic channel depends crucially on the secrecy of the key. The Vernam cipher is the only cipher system which has guaranteed security. In that system the key must be as long as the message and must be used only once. Quantum cryptography is a method whereby key secrecy can be guaranteed by a physical law. So it is impossible, even in principle, to eavesdrop on such channels. Quantum cryptography has been developed in recent years. Up to now, many schemes of quantum cryptography have been proposed[1]-[8]. Now one of the main problems in this field is how to increase transmission distance.

In order to use quantum nature of light, up to now proposed schemes all use very dim light pulses. The average photon number is about 0.1. Because of the loss of the optical fiber, it is difficult for the quantum cryptography based on one photon level or on dim light to realize quantum key-distribution over long distance.

Here we introduce a scheme of quantum cryptography based on coherent state. The average photon number per pulse can be increased, so that we can transmit the key over longer distance.

First of all, we consider the quantum theory of the beam splitter (Fig. 1). Alice sends a mode a_1 which is in state $|\alpha_1\rangle$ into the beam splitter. Bob sends a mode b_1 which is in state $|\beta_1\rangle$ into the BS to measure the state sent by Alice. Suppose the output modes are a_2 and b_2, which are in state $|\alpha_2\rangle$ and $|\beta_2\rangle$ respectively.

According to the quantum theory of BS[9], in Heisenberg picture we have following formula:

$$\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = U \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} U^{+} \tag{1}$$

$$B_{ij} = |B_{ij}| e^{i\phi_{ij}}, \quad \phi_{11} - \phi_{21} = \phi_{12} - \phi_{22} \mp \pi$$

$$|B_{11}|^2 = |B_{22}|^2 = \cos^2\theta, \quad |B_{12}|^2 = |B_{11}|^2 = \sin^2\theta$$

Here U is Unitary Operator of the BS. $\cos^2\theta$ is the reflection rate of the beam splitter.

In Schrödinger picture, if the incoming state is $|\psi_1\rangle = |\alpha_1, \beta_1\rangle$, then the output state $|\psi_2\rangle$ should be

$$|\psi_2\rangle = |\alpha_2, \beta_2\rangle = U^+|\alpha_1, \beta_1\rangle \tag{2}$$

$$U = e^{-iL_2(\phi_r - \phi_\rho)} e^{-i2\cos^{-1}(\tau^{1/2})L_2} e^{-iL_2(\phi_r + \phi_\rho)} \tag{3}$$

$$L_1 = \frac{1}{2}(a_1^+ a_2 + a_2^+ a_1), \quad L_2 = \frac{1}{2i}(a_1^+ a_2 - a_2^+ a_1), \quad L_3 = \frac{1}{2}(a_1^+ a_1 + a_2^+ a_2)$$

$$\phi_r \equiv \frac{1}{2}(\phi_{11} - \phi_{22}), \quad \phi_\rho \equiv \frac{1}{2}(\phi_{11} - \phi_{22} \mp \pi)$$

Using these formula, we can in principle derive the output state for any incoming state. We are particularly interested in the following situation:

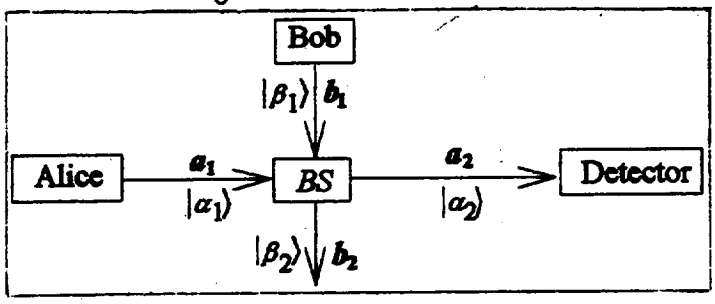

FIG. 1. The basic scheme of quantum cryptography based on coherent states.

Suppose input is a coherent state $|\alpha_1, \beta_1\rangle$. According to above formula, the output state is also a coherent state as following,

$$|\psi_2\rangle = |\alpha_1 \cos\theta - \beta_1 \sin\theta, \beta_1 \cos\theta + \alpha_1 \sin\theta\rangle \equiv |\alpha_2\rangle|\beta_2\rangle \tag{4}$$

$$\alpha_2 = \alpha_1 \cos\theta - \beta_1 \sin\theta, \beta_2 = \beta_1 \cos\theta + \alpha_1 \sin\theta$$

So the output state $|\alpha_2\rangle$ depends on the eigenvalues of incoming coherent states α_1, β_1 and θ. Here $\cos^2\theta$ is the reflection rate of the beam splitter. Now we use a symmetrical beam splitter, $\theta = \frac{\pi}{4}$, and let $\alpha_1 = \alpha$ or $\alpha + \delta\alpha$, $\beta_1 = \alpha$ or $\alpha + \delta\alpha$. In this case, the output state $|\alpha_2\rangle$ is

$$|\alpha_2\rangle = \begin{cases} |0\rangle & \alpha_1 = \beta_1 \\ |\frac{\sqrt{2}}{2}\delta\alpha\rangle & \alpha_1 = \alpha + \delta\alpha, \beta_1 = \alpha \\ |-\frac{\sqrt{2}}{2}\delta\alpha\rangle & \alpha_1 = \alpha, \beta_1 = \alpha + \delta\alpha \end{cases} \tag{5}$$

That means when Alice and Bob send the same coherent state, output state $|\alpha_2\rangle$ is vacuum state $|0\rangle$. When they use different states, $|\alpha_2\rangle$ will be a coherent state and its eigenvalue is proportional to $\pm\frac{\sqrt{2}}{2}\delta\alpha$. Therefore, the probability of detecting photon in state $|\alpha_2\rangle$ is given by this expression,

$$P_n = |\langle n|\alpha_2\rangle|^2 = \begin{cases} 0 & \alpha_1 = \beta_1 \\ e^{-\frac{1}{2}|\delta\alpha|^2} \frac{\delta\alpha/\sqrt{2}}{n!} & \alpha_1 \neq \beta_1 \end{cases} \tag{6}$$

These results tell us when Alice and Bob use the same coherent state, there is no photon to be detected in output state $|\alpha_2\rangle$. Whereas they use different coherent states, the probability of detecting photon is not zero. Now we take the value of $|\delta\alpha|$ is equal to $\sqrt{2\ln 2}$. Then we get

$$\text{when } \alpha_1 = \beta_1, \qquad P_n = 0 \quad (n \geq 1)$$

$$\text{when } \alpha_1 \neq \beta_1, \qquad \begin{cases} P_0 = \frac{1}{2} \\ P = \sum_{n=1}^{\infty} P_n = \frac{1}{2} \end{cases}$$

That means in this case, probability of detecting no photon is 50%, and the other 50% is to detect at least one photon.

Now Alice randomly sends a sequence of coherent states $|\alpha\rangle$ or $|\alpha + \delta\alpha\rangle$, and Bob also randomly use the coherent states $|\alpha\rangle$ or $|\alpha + \delta\alpha\rangle$ to measure the state sent by Alice

Suppose the detecting results after the transmission are shown in Tab.1,

TABLE I. Key distribution using coherent states.

Alice	α	α	$\alpha+\delta\alpha$	α	$\alpha+\delta\alpha$	$\alpha+\delta\alpha$	α	α
Bob	$\alpha+\delta\alpha$	α	α	$\alpha+\delta\alpha$	$\alpha+\delta\alpha$	α	α	$\alpha+\delta\alpha$
detector	Yes	No	Yes	No	No	Yes	No	No
	o	×	o	×	×	o	×	×
Key	1		0			0		

After completing the transmission, Bob announces publicly the cases in which photons are detected, but keeps secret the states he used. Alice and Bob adopt these cases as the key distribution and translate them into a logical 0 or 1 according to their preexitant agreement. For example, Alice's $|\alpha\rangle$ represents a logical 1 and Bob's $|\alpha\rangle$ stands for a logical 0. By far, we have established a shared key distribution between Alice and Bob.

Of course, above results are in the absence of an eavesdropper. Now we consider how to find the eavesdropper in our system if there is. Suppose there is a an eavesdropper named Eve, she wants to split the incoming states $|\alpha_1\rangle$ from Alice and $|\beta_1\rangle$ from Bob into two parts $\{|\alpha_1'\rangle, |\alpha_1''\rangle\}$ and $\{|\beta_1'\rangle, |\beta_1''\rangle\}$ using her beam splitter. Then she sends states $|\alpha_1'\rangle$ and $|\beta_1'\rangle$ to Bob, and keeps states $|\alpha_1''\rangle$ and $|\beta_1''\rangle$ for her own measurement. Repeating above calculation, we can get

$$\alpha_1' = \alpha_1 \cos\varphi, \qquad \alpha_1'' = \alpha_1 \sin\varphi$$

$$\beta_1' = \beta_1 \cos\varphi, \qquad \beta_1'' = \beta_1 \sin\varphi$$

Here $\cos^2\varphi$ is the reflection rate of Eve's beam splitter. We suppose that Bob does the same measurement as before, but in this time he receives the states $|\alpha_1'\rangle$ and $\beta_1'\rangle$ at the beam splitter. When $\alpha_1' \neq \beta_1'$, the probability of detecting photon P' is given by following expression

$$P' = 1 - \exp\{-1/2|\delta\alpha|^2 \cos^2\varphi\} < P \tag{7}$$

Here P is the probability in the absence of an eavesdropper. Now we define a channel disturbance parameter ξ as

$$\xi = \frac{P - P'}{P}$$

In order to check if there is an eavesdropper, they can calculate the channel disturbance parameter ξ after the transmission. If they discover noticeably $\xi > 0$, they can conclude that

there must be an eavesdropper and discard this key distribution. In fact, In order not to been exposed, Eve has to make $\cos\varphi \approx 1$. However, in this case the probability of her detecting photon is

$$P'' = \frac{1}{2}(1 - e^{-\frac{1}{2}|\delta\alpha|^2 \sin^2\varphi}) \approx \frac{1}{4}|\delta\alpha|^2 \sin^2\varphi \approx 0$$

This means that Eve can hardly get any information of the key between Alice and Bob.

Bibliography

[1] S. Wiesner, SIGACT News **15**, 78 (1983).

[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p.175.

[3] C. H. Bennett, G. Brassard, and J. M. Robert, SIAM J. Comput. **17**, 210 (1988).

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvali, and J. Smolin, J. Cryptology **5**, 3 (1991).

[5] A. K. Ekert, Phys. Rev. Lett. **67**, 557 (1991).

[6] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[7] A. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).

[8] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[9] B. Huttner and Y. Ben-Aryeh, Phys. Rev. A **38**, 204 (1988)